



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/696,141	10/25/2000	Paul W. Dent	4015-717	2874
24112	7590	06/17/2004	EXAMINER	
COATS & BENNETT, PLLC			DINH, MINH	
P O BOX 5			ART UNIT	
RALEIGH, NC 27602			PAPER NUMBER	

2132

2

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/696,141

Applicant(s)

DENT, PAUL W.

Examiner

Minh Dinh

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-49 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 31-33 is/are allowed.
- 6) ☐ Claim(s) 1, 2, 4-8, 18, 20, 22-29 and 34-49 is/are rejected.
- 7) ☒ Claim(s) 3, 9-17, 19, 21 and 30 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_.

**DETAILED ACTION**

1. Claims 1-49 have been examined.

***Specification***

2. The disclosure is objected to because of the following informalities: change "orgreater" (page 14, line 4) to "or greater".

Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 5, 12, 28 and 39 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- a. Regarding claim 5, it recites the limitation "changing at least one redundant bit in said ... less than said predetermined value" in the first line. There is insufficient antecedent basis for this limitation in the claim.
- b. Regarding claim 12, it recites the limitation "said error detection bits" in the third line of the claim. There is insufficient antecedent basis for this limitation in the claim.
- c. Regarding claim 28, it recites the limitation "said bit error check" in the second line of the claim. There is insufficient antecedent basis for this limitation in the claim.

d. Regarding claim 39, it recites the limitation "said first predetermined value" in the first line of the claim. There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-2, 4-6, 8, 34-36, 39, and 40-41 rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier ("Applied Cryptography", Section 19.3) in view of Yanovsky (5,703,948).

a. Regarding claim 1, Schneier discloses a method comprising:

comparing a numerical value of a data block, which meets the limitation of an information sequence, to a predetermined value (page 467, "To encrypt a message m ... under 200 digits long.");

if the numerical value of the data block is equal to or greater than the predetermined value, decreasing the size of the data block, which meets the limitation of changing at least one bit in the data block (page 467, "To encrypt a message m ... under 200 digits long.");

encrypting the data block with a key associated with a first modulus (page 467, "To encrypt a message  $m$  ... under 200 digits long.").

Schneier does not teach adding one or more bits to the data block. Yanovsky teaches adding bits to a data block to be transmitted (col. 3, lines 12-15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier to add one or more bits to the data block, as taught by Yanovsky, for error detection and error correction purposes.

b. Regarding claim 2, the bits to be added to the data block as taught by Yanovsky are redundant bits (col. 3, lines 12-15). Please refer to motivation recited for adding more bits to a data block as taught by Yanovsky in claim 1. Schneier further discloses that additional bits can be added to the left of the data block which are the most significant positions (page 467, "(If you need to encrypt ... always be less than  $n$ ).").

c. Regarding claim 4, Schneier further discloses that the predetermined value is the first modulus (page 467, "To encrypt a message  $m$  ... under 200 digits long.").

d. Regarding claim 5, the limitation "at least one redundant bit" is interpreted as "at least one bit" (see claim 1, 8<sup>th</sup> line). Claim 5 is rejected on the same basis as claim 1.

e. Regarding claim 6, the bits to be added to the data block as taught by Yanovsky are error detection bits (col. 3, lines 12-15). Please refer to motivation recited for adding more bits to a data block as taught by Yanovsky in claim 1.

f. Regarding claim 8, Schneier further discloses that the encryption key is a private key (page 467, "The message could just as ... the choice is arbitrary.").

g. Regarding claim 34, Schneier discloses an encryption device comprising:

means for reducing the size of a data block, which meets the limitation of altering a predetermined bit in the data block, if the value of the data block is greater than or equal to a predetermined value (page 467, "To encrypt a message  $m$  ... under 200 digits long.");

a cryptographic processor to encrypt the data block (page 469, RSA in Hardware).

Schneier does not disclose an error encoder to produce an encoded message having one or more error detection bits. Yanovsky discloses an error encoder to produce an encoded message having one or more error detection bits (col. 3, lines 12-15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schneier to include an error encoder, as taught by Yanovsky, in order to produce error detection bits which would be used at the receiving side for detecting transmission errors. Accordingly, the error encoder should comprise the means for reducing the size of data blocks discussed above so that the data blocks are ready for encryption.

h. Regarding claim 35, Schneier further discloses that the cryptographic processor encrypts the data block using a first encryption key associated with a first modulus (page 467, "To encrypt a message  $m$  ... under 200 digits long.").

i. Regarding claim 36, Schneier further discloses that the first encryption key is a private key of the sender of the data block (page 467, "The message could just as ... the choice is arbitrary.").

j. Regarding claim 39, the limitation "said first predetermined value" is interpreted as "said predetermined value" (see Claim 34, 5<sup>th</sup> line). Schneier further discloses that the predetermined value is equal to the first modulus (page 467, "To encrypt a message m ... under 200 digits long."). Although Schneier does not disclose the feature "less one", the predetermined value in the Schneier method and the predetermined value of the claim are functionally equivalent.

k. Regarding claim 40, Schneier further discloses that the data block is not changed when its value is less than the predetermined value (page 467, "To encrypt a message m ... under 200 digits long.").

l. Regarding claim 41, Schneier does not explicitly disclose a transmitter. However, this feature is deemed inherent to the Schneier device since page 471 (see Scenario 1) shows that the message is transmitted. The Schneier device would be inoperative if there were no transmitter.

7. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Yanovsky as applied to claim 6 above, and further in view of "Computer Dictionary". Schneier and Yanovsky do not disclose computing a cyclic redundancy check code and appending the cyclic redundancy check code to the data block. The "Computer Dictionary" discloses computing a cyclic redundancy check code and appending the cyclic redundancy check code to the data block (pages 122-123). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier and Yanovsky to include computing a cyclic

redundancy check code and appending the cyclic redundancy check code to the data block, as taught in the "Computer Dictionary", so that the receiving side could use the cyclic redundancy check code to detect transmission errors.

8. Claims 18, 20, 22 and 42-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier ("Applied Cryptography", Sections 2.7 and 19.3) in view of Yanovsky.

a. Regarding claim 18, Schneier discloses a method comprising:

comparing a value of a data block, which meets the limitation of an information sequence, with a value of a first modulus and decreasing the size of the data block if the data block is equal to or greater than the first modulus (page 467, "To encrypt a message  $m$  ... under 200 digits long.");

signing the data block with a first key based on the first modulus to form a signed message (page 467, "The message could just as ... the choice is arbitrary.");

sending the signed message to a recipient (page 467, "The message could just as ... the choice is arbitrary.").

Schneier does not teach appending one or more redundant bits to the data block. Yanovsky teaches appending redundant bits to a data block to be transmitted (col. 3, lines 12-15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier to append one or more redundant bits to the data block, as taught by Yanovsky, for error detection and error correction purposes.



Section 19.3 of the "Applied Cryptography" reference does not disclose encrypting the signed message with a second key based on a second modulus. However, Schneier, in Section 2.7, teaches encrypting a digital signature with a second key based on a second modulus (page 41, "By combining digital signatures ... and sends it to Bob."). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier disclosed in Section 19.3 to encrypt the signed message with a second key based on a second modulus, as taught in Section 2.7, in order to combine the security of encryption with the authenticity of digital signatures.

b. Regarding claim 20, Schneier further discloses that the first key is the sender's private key (page 467, "The message could just as ... the choice is arbitrary.").

c. Regarding claim 22, the redundant bits to be added to the data block as taught by Yanovsky are error detection bits (col. 3, lines 12-15). Please refer to motivation recited for adding more bits to a data block as taught by Yanovsky in claim 18.

d. Regarding claim 42, Schneier discloses a device comprising:

A cryptographic processor to decipher an encrypted bit string to obtain a plaintext message, wherein the cryptographic processor uses a key associated with a modulus for a decryption operation (page 467, "To decrypt a message, take each ... the choice is arbitrary."; and page 469, RSA in Hardware).

Section 19.3 of the "Applied Cryptography" reference does not disclose that the message is doubly encrypted and the cryptographic processor uses a second key associated with a second modulus for a second decryption operation. However,

Schneier, in Section 2.7, discloses a doubly encrypted message and two decryption operations using a first key associated with a first modulus and a second key associated with a second modulus to retrieve the plaintext message (page 41, "By combining digital signatures ... and recovers the message."). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schneier disclosed in Section 19.3 to receive a doubly encrypted message and perform two decryption operations using a first key associated with a first modulus and a second key associated with a second modulus, as taught in Section 2.7, in order to combine the security of encryption with the authenticity of digital signatures.

Schneier does not disclose a decoder comprising a bit alteration detector to detect whether a predetermined bit of the transmitted message was altered. Yanovsky discloses a decoder comprising a bit alteration detector to detect whether a predetermined bit of the transmitted message was altered and perform correction if error was detected (col. 3, lines 1-5, 10-14; col. 5, lines 8-13). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schneier such that it includes a decoder comprising a bit alteration detector to detect whether a predetermined bit of the transmitted message was altered and perform correction if error was detected, as taught by Yanovsky, in order to detect and correct transmission errors in the random bit of the transmitted message.

e. Regarding claims 43-49, the features of the claims are directed to detecting and correcting transmission errors. Yanovsky further discloses detecting and correcting

transmission errors (col. 3, lines 10-14; col. 5, lines 7-13). Please refer to motivation recited in claim 42.

9. Claims 23-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier ("Applied Cryptography", Section 2.7) in view of Yanovsky.

a. Regarding claim 23, Schneier discloses a method for deciphering a doubly encrypted bit string comprising:

deciphering the doubly encrypted bit string to obtain a once encrypted bit string (page 41, "By combining digital signatures ... recovers the message.");

deciphering the once encrypted bit string to obtain a plain text message (page 41, "By combining digital signatures ... recovers the message.").

Schneier does not disclose using error detection bits to determine whether a predetermined bit in the message was altered. Yanovsky discloses adding error detection and error correction bits to a message at the transmitting side and, at the receiving side, performing a bit alteration check using the added bits to determine whether a predetermined bit in the message was altered and provide correction if errors are found (col. 3, lines 1-5, 12-15; col. 5, lines 8-13). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier to perform a bit alteration check, at the receiving side, using the error detection and error correction bits generated at the transmitting side, to determine whether a predetermined bit in the message was altered and provide correction if errors

Art Unit: 2132

are found, as taught by Yanovsky, so that transmission errors in a random bit could be detected and corrected.

b. Regarding claim 24, Yanovsky further discloses that performing bit alteration check comprises correcting errors in the predetermined bit (col. 3, lines 12-15; col. 5, lines 8-13). Please refer to motivation recited for performing a bit alteration check as taught by Yanovsky in claim 23.

c. Regarding claim 25, Yanovsky further discloses that performing bit alteration check comprises checking for a bit error in a predetermined position (col. 3, lines 12-15; col. 5, lines 8-13). Please refer to motivation recited for performing a bit alteration check as taught by Yanovsky in claim 23.

d. Regarding claims 26-27, Yanovsky further discloses that performing bit alteration check comprises determining the value of a bit in the predetermined position and correcting the value if there is a transmission error (col. 3, lines 12-15; col. 5, lines 8-13). Please refer to motivation recited for performing a bit alteration check as taught by Yanovsky in claim 23.

e. Regarding claims 28 and 29, the claims are directed to detecting and correcting transmission errors. Yanovsky further discloses detecting and correcting transmission errors (col. 3, lines 12-15; col. 5, lines 8-13). Please refer to motivation recited in claim 23.

10. Claims 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier ("Applied Cryptography", Section 19.3) in view of Yanovsky as applied to claim

35 above, and further in view of Schneier ("Applied Cryptography", Section 2.7).

Section 19.3 of the "Applied Cryptography" reference does not disclose encrypting the encrypted message with a second key associated with a second modulus and the second key being a public key of the recipient of the message. However, Schneier, in Section 2.7, teaches encrypting a digital signature with a second key associated with a second modulus and the second key being a public key of the recipient of the message (page 41, "By combining digital signatures ... and sends it to Bob."). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schneier disclosed in Section 19.3 to encrypt the signed message with a second key associated with a second modulus and the second key being a public key of the recipient of the message, as taught in Section 2.7, in order to combine the security of encryption with the authenticity of digital signatures.

***Allowable Subject Matter***

11. Claims 3, 9-17, 19, 21, 30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The following is a statement of reasons for the indication of allowable subject matter.

a. Regarding claim 3, the feature of the claim, changing the redundant bit at the most significant bit position, in combination with elements of the parent claims have not been taught by prior art.

Art Unit: 2132

b. Regarding claim 9, the feature of the claim, a second modulus less than the first modulus, in combination with elements of the parent claims have not been taught by prior art.

c. Regarding claim 19, the feature of the claim, appending one or more redundant bits to an information sequence comprises forming a message having a length equal to the first modulus, in combination with elements of the parent claims have not been taught by prior art.

d. Regarding claim 21, the feature of the claim, changing the value of one of the redundant bits, in combination with elements of the parent claims have not been taught by prior art.

e. Regarding claim 30, the feature of the claim, adding a value equal to a modulus associated with an encryption key used to generate the doubly encrypted bitstring, in combination with elements of the parent claims have not been taught by prior art.

12. Claims 31-33 are allowed. The following is an examiner's statement of reasons for allowance. Claim 31 is directed to a method of decrypting a doubly encrypted bit string. More specifically, the claim identifies the uniquely distinct feature: modifying the once encrypted bit string by adding an integer multiple of a modulus associated with an encryption key used to generate the doubly encrypted bit string to the once encrypted bit string to obtain a modified once encrypted bit string. The closest prior art, Schneier ("Applied Cryptography"), also disclose a method of decrypting a doubly encrypted bit string. However, Schneier does not teach modifying the once encrypted bit string. The

prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

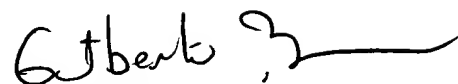
Application/Control Number: 09/696,141  
Art Unit: 2132

Page 15

MD

Minh Dinh  
Examiner  
Art Unit 2132

MD  
6/10/2004



GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100